THOMPSON'S HACKING SCHEME

1. THOMPSON SCANS AWS CLIENTS' PUBLIC-FACING SERVERS

| Properly Configured Server | Properly Configured Server | Properly Configured Server | **Server with Misconfigured Web Application Firewall** | Properly Configured Server | Properly Configured Server | Properly Configured Server |
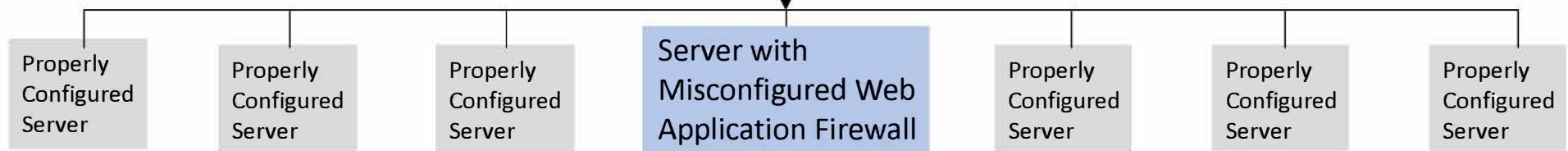
2. THOMPSON IDENTIFIES ROLE ("iam/role")

- NAME OF ROLE

3. THOMPSON STEALS CREDENTIALS FOR ROLE ("GET . . . iam/security credentials/[role]")

- ACCESS KEY
- SECRET ACCESS KEY
- TOKEN

4. THOMPSON USES STOLEN CREDENTIALS TO ASSUME ROLE

| If role can read and copy data, Thompson steals data (*e.g.,* Capital One) | If role can do both, Thompson steals data and mines cryptocurrency (*e.g.,* Victim 7) | If role can create new servers, Thompson mines cryptocurrency |